

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-344924**  
(43)Date of publication of application : **29.11.2002**

(51)Int.CI. H04N 7/167  
H04L 9/08

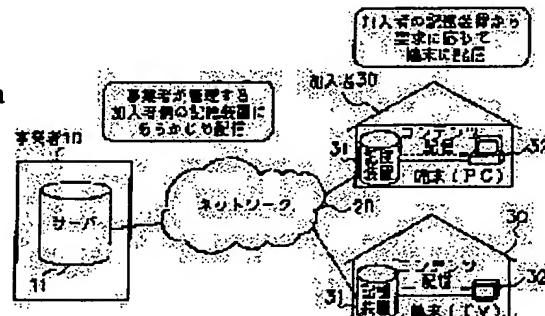
(21)Application number : 2001-152371 (71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>  
(22)Date of filing : 22.05.2001 (72)Inventor : TOMONOBU KIMITAKA  
YAMAMOTO TAKESHI

## (54) CONTENTS DISTRIBUTION METHOD AND ITS APPARATUS

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a contents distribution method and its apparatus that can transfer contents in advance to a subscriber and allow an enterprise to manage its release time.

**SOLUTION:** A server 11 of an enterprise 10 distributes encrypted contents to a data storage device 31 placed at a subscriber side 30 or part of its areas via a network 20 before a release time set to the encrypted contents in advance by the enterprise, when the release time comes or when a time receiving a use request of the encrypted contents from the subscriber side exceeds the release time, the enterprise 10 distributes an encryption key of the encrypted contents from the enterprise 10 to the subscriber 30 so as to distribute a load of the server and the network attended with distribution of contents with a large capacity to a plurality of subscribers, illegal use of the contents can be prevented so as to attain simultaneous use by a plurality of subscribers.



## LEGAL STATUS

[Date of request for examination] 10.10.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

### Number of appeal against examiner's decision of

rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-344924  
(P2002-344924A)

(43) 公開日 平成14年11月29日 (2002.11.29)

(51) Int.Cl.<sup>7</sup>  
H 04 N 7/167  
H 04 L 9/08

識別記号

F I  
H 04 N 7/167  
H 04 L 9/00  
Z 5 C 0 6 4  
6 0 1 A 5 J 1 0 4  
6 0 1 B  
6 0 1 E

テ-マコ-ト (参考)

(21) 出願番号 特願2001-152371 (P2001-152371)

(22) 出願日 平成13年5月22日 (2001.5.22)

(71) 出願人 000004226  
日本電信電話株式会社  
東京都千代田区大手町二丁目3番1号  
(72) 発明者 友信 公孝  
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
(72) 発明者 山本 剛  
東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
(74) 代理人 100069981  
弁理士 吉田 精孝

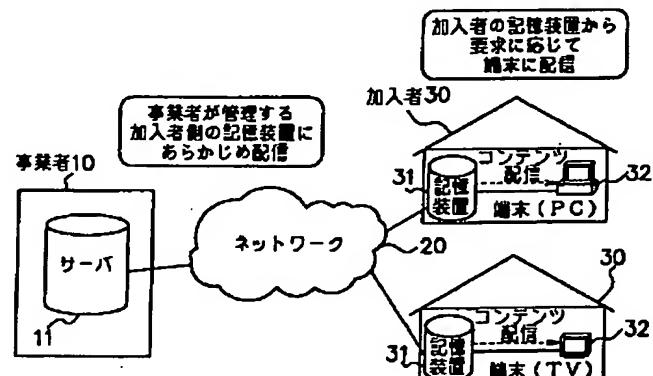
最終頁に続く

(54) 【発明の名称】 コンテンツ配信方法及びその装置

(57) 【要約】

【課題】 コンテンツを予め加入者側へ配信でき、しかもその使用解禁時刻を事業者側で管理できるコンテンツ配信方法及びその装置を提供すること。

【解決手段】 事業者10のサーバ11からネットワーク20を介して暗号化コンテンツを予め、加入者30側に配置したデータ記憶装置31あるいはその領域の一部に、当該暗号化コンテンツに対して事業者が設定した使用解禁時刻以前に配信するとともに、前記使用解禁時刻になった時もしくは加入者側からの当該暗号化コンテンツの利用要求を受け付けた時の時刻が前記使用解禁時刻を経過していれば、事業者10から加入者30へ前記暗号化コンテンツの暗号鍵を配信することにより、大容量コンテンツの複数加入者への配信に伴うサーバやネットワークの負荷を分散可能とし、かつコンテンツの不正使用を防止し、複数加入者での同時使用を可能とする。



## 【特許請求の範囲】

【請求項 1】 コンテンツを提供する事業者からコンテンツを利用する加入者へ暗号化した暗号化コンテンツ及び該暗号化コンテンツを解読するための暗号鍵をネットワークを介して配信し、加入者は前記暗号鍵により前記暗号化コンテンツを解読して利用するコンテンツ配信方法において、

前記暗号化コンテンツを予め、加入者側に配置したデータ記憶装置あるいはその領域の一部に、当該暗号化コンテンツに対して事業者が設定した使用解禁時刻以前に配信するとともに、

前記使用解禁時刻になった時、前記暗号化コンテンツの暗号鍵を配信することを特徴とするコンテンツ配信方法。

【請求項 2】 前記使用解禁時刻になった時、前記暗号鍵を 2 以上の加入者へ同報配信することを特徴とする請求項 1 記載のコンテンツ配信方法。

【請求項 3】 コンテンツを提供する事業者からコンテンツを利用する加入者へ暗号化した暗号化コンテンツ及び該暗号化コンテンツを解読するための暗号鍵をネットワークを介して配信し、加入者は前記暗号鍵により前記暗号化コンテンツを解読して利用するコンテンツ配信方法において、

前記暗号化コンテンツを予め、加入者側に配置したデータ記憶装置あるいはその領域の一部に、当該暗号化コンテンツに対して事業者が設定した使用解禁時刻以前に配信するとともに、

事業者が加入者からの当該暗号化コンテンツの利用要求を受け付けた時の時刻が前記使用解禁時刻を経過していれば、前記暗号化コンテンツの暗号鍵を当該加入者へ配信することを特徴とするコンテンツ配信方法。

【請求項 4】 加入者からの暗号化コンテンツの利用要求を受け付けた時の時刻が前記使用解禁時刻を経過していない場合、事業者は当該加入者へ不許可を通知することを特徴とする請求項 3 記載のコンテンツ配信方法。

【請求項 5】 1 つの暗号化コンテンツの 2 以上の部分に対してそれぞれ異なる使用解禁時刻を設定したことを特徴とする請求項 1 乃至 4 いずれか記載のコンテンツ配信方法。

【請求項 6】 前記データ記憶装置あるいはその領域の一部に、暗号化しておらず、使用解禁時刻を設定していないコンテンツを配信することを特徴する請求項 1 乃至 5 いずれか記載のコンテンツ配信方法。

【請求項 7】 コンテンツを提供する事業者からコンテンツを利用する加入者へ暗号化された暗号化コンテンツ及び該暗号化コンテンツを解読するための暗号鍵をネットワークを介して配信し、加入者は前記暗号鍵により前記暗号化コンテンツを解読して利用するコンテンツ配信装置において、

加入者が使用する加入者側装置と、事業者が使用する事

業者側装置と、これらを接続するネットワークとからなり、

加入者側装置は、

暗号化コンテンツを記憶するデータ記憶装置と、データ記憶装置に記憶された暗号化コンテンツを暗号鍵により解読する手段と、

解読されたコンテンツを利用する手段とを備え、

事業者側装置は、

暗号化コンテンツを当該暗号化コンテンツに対して設定した使用解禁時刻以前に加入者側装置のデータ記憶装置あるいはその領域の一部に配信する手段と、

現在の時刻と前記使用解禁時刻とを照合し、前記使用解禁時刻になった時、前記暗号化コンテンツの暗号鍵を加入者側装置へ配信する手段とを備えたことを特徴とするコンテンツ配信装置。

【請求項 8】 事業者側装置は、前記使用解禁時刻になった時、前記暗号化コンテンツの暗号鍵を 2 以上の加入者側装置へ同報配信する手段を備えたことを特徴とする請求項 7 記載のコンテンツ配信装置。

【請求項 9】 コンテンツを提供する事業者からコンテンツを利用する加入者へ暗号化された暗号化コンテンツ及び該暗号化コンテンツを解読するための暗号鍵をネットワークを介して配信し、加入者は前記暗号鍵により前記暗号化コンテンツを解読して利用するコンテンツ配信装置において、

加入者が使用する加入者側装置と、事業者が使用する事業者側装置と、これらを接続するネットワークとからなり、

加入者側装置は、

暗号化コンテンツを記憶するデータ記憶装置と、暗号化コンテンツの利用を事業者側装置に対して要求する手段と、

データ記憶装置に記憶された暗号化コンテンツを暗号鍵により解読する手段と、

解読されたコンテンツを利用する手段とを備え、

事業者側装置は、

暗号化コンテンツを当該暗号化コンテンツに対して設定した使用解禁時刻以前に加入者側装置のデータ記憶装置あるいはその領域の一部に配信する手段と、

加入者側装置からの暗号化コンテンツの利用要求を受け付ける手段と、

前記利用要求を受け付けた時の時刻と前記使用解禁時刻とを照合し、前記使用解禁時刻を経過していれば、前記暗号化コンテンツの暗号鍵を当該加入者側装置へ配信する手段とを備えたことを特徴とするコンテンツ配信装置。

【請求項 10】 前記利用要求を受け付けた時の時刻が前記使用解禁時刻を経過していない場合、当該加入者側装置へ不許可を通知する手段を備えたことを特徴とする請求項 9 記載のコンテンツ配信装置。

【請求項11】 1つの暗号化コンテンツの2以上の部分に対してそれぞれ異なる使用解禁時刻を設定したことと特徴とする請求項7乃至10いずれか記載のコンテンツ配信装置。

【請求項12】 事業者側装置は、暗号化しておらず、使用解禁時刻を設定していないコンテンツを加入者側装置のデータ記憶装置あるいはその領域の一部に配信する手段を備えたことを特徴する請求項7乃至11いずれか記載のコンテンツ配信装置。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】 本発明は、事業者から加入者へコンテンツをネットワークを介して配信する方法、特にコンテンツを予め加入者側へ配信でき、しかもその使用解禁時刻を事業者側で管理できるコンテンツ配信方法及びその装置に関するものである。

##### 【0002】

【従来の技術】 従来の映像等のギガビットクラスのコンテンツ配信方法は、図1に示すように、インターネットプロバイダ、コンテンツプロバイダ、データセンタ等の事業者1側に配置された該映像等のギガビットクラスのコンテンツを記憶するサーバ2から、加入者3側に配置されたパーソナルコンピュータ(PC)、テレビジョン受信機(TV)等の端末4へネットワーク5を介して、事業者1が定めた時間に一方的かつストリーム的にブロードキャスト及びマルチキャストで配信する方法であった。

【0003】 また、従来のオンデマンド型配信は、加入者が希望のコンテンツを要求する信号を事業者に送信し、該加入者の要求に応じて事業者のサーバから加入者にコンテンツを配信する方法であった。

【0004】 従来の技術において、コンテンツが加入者側の記憶装置あるいはその領域の一部に蓄積されると、使用開始までの時間的な制限はなく、コンテンツを入手すると、加入者は認証等の作業を行った後に、コンテンツを自由に使用開始することが可能である。

【0005】 このように、従来技術では、コンテンツを予め配信した場合、通常のテレビ放送やラジオ放送のように、各加入者におけるコンテンツの使用を同時とさせることが困難であり、また、使用解禁時間が未来に定められているコンテンツを事業者が配信することはない。

【0006】 一方、従来のテレビ放送やラジオ放送を記録するためには、予め放送を記録する予約設定を記録装置にしなければならず、放送終了後に記録することはできない。

##### 【0007】

【発明が解決しようとする課題】 ネットワークが大容量化され、ディジタルテレビ放送等をネットワークで配信することが現実的になっている。しかし、ネットワークが大容量化されても、サーバの送信容量はネットワーク

に対応して大容量化されておらず、ギガビットクラスの大容量コンテンツを配信するにはサーバの負荷が大きいことが課題である。

【0008】 従来の技術において、ネットワークでコンテンツをストリーム的に配信する方法は、ネットワークへの負荷が大きい。また、広帯域ネットワークを使用しても、一度に非常に多くの加入者がアクセスすると、ネットワークやサーバへの負荷が大きくなることが課題である。

【0009】 従来の技術において、加入者の希望に応じて配信するオンデマンド型配信や、コンテンツをまとめて配信するブロック型配信では、同時に複数の加入者がコンテンツを使用することはない。

【0010】 従来の技術において、事業者がコンテンツを加入者に一旦配信すると、事業者がコンテンツの使用解禁時刻等を管理することは困難であり、そのため不正コピー等による著作権が侵害されることが問題である。

【0011】 従来の技術においては、ネットワークのトラフィック量は昼間が多く、深夜は昼間に比べると非常に少ない。このように、トラフィック量は時間により偏っていることが問題である。

【0012】 従来のテレビやラジオ放送を予め記録する予約設定を忘れた場合や誤った設定を行った場合には、事業者側が決定する時間に放送される再放送を待つか、他人が記録したものを得るしかないことが問題である。

【0013】 本発明の目的は、コンテンツを予め加入者側へ配信でき、しかもその使用開始時刻を事業者側で管理できるコンテンツ配信方法及びその装置を提供することにある。

##### 【0014】

【課題を解決するための手段】 前記目的を達成するため、本発明では、コンテンツを提供する事業者からコンテンツを利用する加入者へ暗号化した暗号化コンテンツ及び該暗号化コンテンツを解読するための暗号鍵をネットワークを介して配信し、加入者は前記暗号鍵により前記暗号化コンテンツを解読して利用するコンテンツ配信方法において、前記暗号化コンテンツを予め、加入者側に配置したデータ記憶装置あるいはその領域の一部に、当該暗号化コンテンツに対して事業者が設定した使用解禁時刻以前に配信するとともに、前記使用解禁時刻になった時、前記暗号化コンテンツの解読鍵を配信することを特徴とする。

【0015】 従来の技術とは、コンテンツの使用開始が許可される以前にコンテンツを配信可能であり、ネットワークやサーバへの負荷を小さくできるとともに、加入者がコンテンツを不正に使用することを防ぎ、著作権を保護して使用することが可能である点が異なる(請求項1、7)。

【0016】 また、前記発明において、前記使用解禁時

刻になった時、前記暗号鍵を2以上の加入者へ同報配信することを特徴とする。

【0017】従来の技術とは、予め配信したコンテンツを、各加入者が同時に使用を開始することが可能である点が異なる（請求項2、8）。

【0018】また、コンテンツを提供する事業者からコンテンツを利用する加入者へ暗号化した暗号化コンテンツ及び該暗号化コンテンツを解読するための暗号鍵をネットワークを介して配信し、加入者は前記暗号鍵により前記暗号化コンテンツを解読して利用するコンテンツ配信方法において、前記暗号化コンテンツを予め、加入者側に配置したデータ記憶装置あるいはその領域の一部に、当該暗号化コンテンツに対して事業者が設定した使用解禁時刻以前に配信するとともに、事業者が加入者からの当該暗号化コンテンツの利用要求を受け付けた時の時刻が前記使用解禁時刻を経過していれば、前記暗号化コンテンツの暗号鍵を当該加入者へ配信することを特徴とする。

【0019】従来の技術とは、予め配信したコンテンツを、加入者からの要求に応じて、使用開始時刻を経過している場合のみ、利用可能とする点が異なる（請求項3、9）。

【0020】また、前記発明において、加入者からの暗号化コンテンツの利用要求を受け付けた時の時刻が前記使用解禁時刻を経過していない場合、事業者は当該加入者へ不許可を通知することを特徴とする。

【0021】従来の技術とは、加入者からの要求が使用解禁時刻以前であれば、不許可を通知し、予め配信したコンテンツを利用させない点が異なる（請求項4、10）。

【0022】また、前記発明において、1つの暗号化コンテンツの2以上の部分に対してそれぞれ異なる使用解禁時刻を設定したことを特徴とする。

【0023】従来の技術とは、暗号化コンテンツを2以上の部分毎に利用を管理できる点が異なる（請求項5、11）。

【0024】また、前記発明において、前記データ記憶装置あるいはその領域の一部に、暗号化しておらず、使用解禁時刻を設定していないコンテンツを配信することを特徴する。

【0025】従来の技術とは、予め配信したコンテンツを、事業者の許可を得ることなく、加入者が自由に使用することが可能である点が異なる（請求項6、12）。

【0026】このように、本発明によれば、大容量のコンテンツを予め、即ち当該コンテンツの使用解禁時刻以前に加入者側の記憶装置あるいはその領域の一部に配信することで、コンテンツを配信するサーバの負荷が軽減され、また、トラフィック量の少ない時間帯に配信すればトラフィック量が時間的に分散され、ネットワークを有効に活用することができる。また、コンテンツの使用

解禁時刻を事業者側で管理可能とすることにより、予め配信されたコンテンツを加入者が不正に使用することなく、著作権を保護して加入者がコンテンツを使用することが可能である。これにより、加入者は従来のTV放送やラジオ放送との違いを意識することなく、各加入者が同時にTV番組やラジオ放送のコンテンツを視聴することが可能となる。

【0027】

【発明の実施の形態】以下、本発明の実施の形態の一例を図面を参照して説明する。

【0028】ここではコンテンツとして、ギガビットクラスのデータの映像を例にとり、ネットワークを介して配信する方法を説明する。

【0029】まず、ネットワーク構成とコンテンツ配信方法の概念について述べる。

【0030】従来のネットワークを介して配信する放送は、図1に示したように、事業者1側に配置されていたサーバ2からコンテンツを、事業者の定めた時間にストリーム的に配信する。

【0031】それに対して、本発明による配信方法では、図2に示すように、事業者1のサーバ11から暗号化したコンテンツを予め、該コンテンツの使用解禁時刻以前にネットワーク20を介して、各加入者30側に配置したデータ記憶装置31あるいはその領域の一部に配信する。そして、コンテンツの放送開始時刻（使用解禁時刻）になると、図3に示すように、暗号を解読するための暗号鍵41を各加入者30に同報配信し、この暗号鍵41により解読したコンテンツを加入者の端末32で使用する。

【0032】このように、加入者側に配置した記憶装置あるいはその領域の一部、並びに予め配信したコンテンツの使用許可の権限は事業者が管理しており、使用解禁時刻以前に加入者が不正にコンテンツを使用することを防ぎ、コンテンツの著作権を保護できる。

【0033】具体的な配信方法について説明する。

【0034】現在のテレビ放送のコンテンツは、スポーツや音楽ライブの生中継等の予め蓄積できないコンテンツと、ドラマや過去のスポーツ等の既に録画した蓄積型のコンテンツとに大別できる。前者は現場から生放送する必要があるが、後者は加入者に対してテレビ放送局等の事業者が定めた放送時間通りに配信する必要はない。

【0035】そこで、蓄積型のコンテンツについて述べる。本発明では、事業者が定めた放送開始時刻以前に、加入者側の記憶装置あるいはその領域の一部に、暗号化処理を施した暗号化コンテンツを予め配信する。事業者が予め配信する暗号化コンテンツの容量は、加入者側の記憶装置あるいはその領域の一部の容量に応じて数時間分から数日分である。

【0036】配信する時間帯は、トラフィック量の少ない深夜にかけて行う。また、配信する方法は、一度に全

での加入者に配信するのではなく、ネットワークに負荷をかけない程度の数の加入者側装置に対して配信を行う。

【0037】加入者側装置は、コンテンツを使用するに際し、要求信号を事業者側装置に送信する。この要求信号には、加入者の情報及びコンテンツの任意の要求箇所等の情報が含まれる。

【0038】また、事業者側装置は、加入者側装置内のコンテンツを定期的に更新する。加入者側には未放送分のコンテンツを数時間分あるいは数日分配しておく。この書き換えは加入者側装置の要求信号に応じて行う場合もある。

【0039】次に、予め配信されたコンテンツを加入者側装置が使用する方法について述べる。

【0040】予め配信されたコンテンツの種類に応じて、事業者がコンテンツの使用開始時刻（使用解禁時刻）、使用期間、使用終了時刻を設けているものと、それらの制限がなく自由に使用できるものとの2種類がある。

【0041】例えば、後者の自由に使用可能なコンテンツとしてはニュース、天気予報、過去のスポーツ等がある。このコンテンツは、加入者側の記憶装置あるいはその領域の一部に配信された後は、加入者が希望すれば、事業者の許可を得ることなく自由に使用することが可能である。

【0042】それに対し、前者のように、例えばドラマや映画等の使用解禁時刻が設定されているコンテンツを加入者側装置が使用するには、事業者側装置からの使用許可を必要とする。

【0043】使用を制限する方法として、例えば図4に示すように、コンテンツに暗号化を施しておき、加入者30側の記憶装置31が要求信号を事業者10側のサーバ11に送信し、認証された時のみ、事業者側のサーバ11が暗号を解読する暗号鍵41を配信する方法がある。

【0044】この暗号鍵は多くの加入者が使用するが、不正使用防止の観点から共通鍵を使用する。この暗号鍵は事業者側装置（サーバ）が管理しており、コンテンツの使用の許可などの権限は事業者側にある。このため、加入者側装置（加入者）は事業者側の許可なくコンテンツを不正に使用することは出来ない。

【0045】暗号鍵の配信方法は、加入者側装置からの要求信号を事業者が許可した時、一度だけ配信する方法がある。この方法では、加入者側装置では暗号解除ソフトウェアが受信した暗号鍵を用いてコンテンツの暗号を解除する。

【0046】また、コンテンツを暗号化する方法として、暗号化のアルゴリズムに従い暗号鍵を一定周期毎に変更する（コンテンツ毎に変更、コンテンツの2以上の部分毎に変更等）方法がある。一定周期毎に異なる暗号

鍵で暗号化されたコンテンツは、事業者側装置から予め加入者側装置に配信する。

【0047】次に、暗号の解除方法について説明する。

【0048】加入者側装置が要求信号を送信し、事業者がコンテンツの使用を許可した場合、暗号化と同じ周期毎に事業者側装置から各加入者側装置に暗号鍵を配信する。加入者側装置では一定周期毎に暗号鍵を受信し、暗号解除ソフトウェアがコンテンツを解除し、コンテンツの使用が可能になる。

【0049】図5に暗号を解除する方法を示す。加入者側装置内に配信された暗号化されたコンテンツ42と、事業者側から送信された暗号を解除する鍵41とを暗号解除回路33に入力し、コンテンツに施された暗号を解除する。暗号解除回路33からは暗号を解除されたコンテンツ43が出力される。

【0050】また、他の暗号化方法として、図6に示すように、例えば映像の1コマ毎あるいは数コマ毎に異なる一部が欠けた映像51を予め配信しておき、加入者がコンテンツを使用する時に、事業者から残りの一部の映像を連続的に暗号鍵として送信する方法がある。

【0051】また、各加入者へ配信するコンテンツを異なる共通鍵を用いて暗号化し、該加入者毎に異なる共通鍵（を加入者毎に異なる公開鍵で暗号化した上で）を配信する方法もある。

【0052】暗号解除方法を図7に示す。加入者側装置内において、予め蓄積された暗号化された映像51と新たに事業者側装置から送信された映像52を、暗号解除回路33に入力する。暗号解除回路33は、それらの映像を合成することで暗号化を解除し、加入者側端末に出力する（53）。

【0053】暗号鍵を用いる方法としては、このように3通りの方法が考えられる。但し、コンテンツの不正使用を防止する観点からは、事業者がコンテンツの使用を許可した時の一度だけ暗号鍵を送信する場合に比べて、数秒毎あるいは連続的に暗号鍵を送信するほうが望ましい。また、予め配信されたコンテンツを不正に使用されないように、暗号を解読する鍵は事業者側装置内で管理し、加入者が簡単に解読できない、数十ビットから百数十ビットから構成される暗号技術を使用する必要がある。

【0054】このように、加入者側の記憶装置あるいはその領域の一部並びに予め配信したコンテンツの使用許可を与える暗号鍵を事業者が管理することで、加入者側装置においてコンテンツを不正に使用することを防ぐことが可能である。また、これにより著作権を保護することが可能である。

【0055】加入者側装置が要求信号を送出した場合の認証方法は、加入者側装置固有の情報、事業者が割り当てた加入者の情報（ユーザID）及びパスワード等の組み合わせ等を用いて認証する。また、認証時に、どのコ

ンテンツを利用するかを事業者側が記録し、データベース化すると、事業者側は加入者側の嗜好を把握でき、加入者側の好む内容を通知するサービスを行うことが可能である。

【0056】事業者側装置が共通鍵を配信する方法は、共通鍵自身にも加入者固有の公開鍵で暗号をかけておく。つまり、加入者側装置では、まずコンテンツを使用するための共通鍵を得るため、前記加入者固有の公開鍵とペアの秘密鍵を用いて暗号を解除する。そして得られた共通鍵を用いて、配信されたコンテンツの暗号化を解除し、コンテンツを使用することが可能になる。

【0057】図8は事業者側装置（サーバ）の構成の一例を示すもので、図中、111は記憶装置、112は送受信回路、113は認証回路、114は時間管理回路、115は鍵送信回路、116は加入者データベース、117は暗号化回路である。

【0058】記憶装置111は、コンテンツを蓄積し、要求があれば蓄積したコンテンツを出力する。送受信回路112は、コンテンツを加入者側に送信し、加入者側装置からの要求信号を受信する。認証回路113は、加入者の識別情報、パスワード及び加入者側装置の識別情報等を用いて各加入者の認証作業を行う。

【0059】時間管理回路114は、現在時刻を管理しており、加入者側装置からの要求信号が到着した時刻または要求箇所の時刻と現在時刻との関係から、コンテンツの使用許可あるいは不許可を判定する。許可した場合は、鍵送信回路115に通知する。また、各加入者に配信したコンテンツを使用する有効期限も管理しており、有効期限を経過したコンテンツに対しては許可を与えない。

【0060】有効期限を経過した加入者側装置内のコンテンツは、事業者側装置が削除するか、新たなコンテンツを上書きすることで速やかに消去する。

【0061】鍵送信回路115は、時間管理回路114から許可判定信号が通知されると、送受信回路112を介して暗号鍵を加入者側装置に配信する。

【0062】加入者データベース116は、加入者が選択するコンテンツから加入者の嗜好情報を蓄積する。それにより、新たなサービスや新たなコンテンツ等の情報を加入者側装置に送信することが可能である。

【0063】暗号化回路117は、記憶装置111から加入者側端末へ送信されるコンテンツを送信前に暗号化処理する。

【0064】また、サーバ11は、一定期間経過したコンテンツ及び有効期限を経過したコンテンツを加入者側の記憶装置あるいはその領域の一部から削除する。

【0065】次に、加入者が事業者に要求を出した時の、事業者がコンテンツの使用許可または不許可を与える時間的流れについて説明する。

【0066】図9に、コンテンツの時間的な使用可能領

域を示す。事業者側の装置は、常に現在の時刻から使用開始時刻を引いた時間を計算し、現在時刻相当箇所61を認識する。また、コンテンツの先頭62からその時間分経過した位置までを時間的な使用可能領域63として常に把握する。それ以外は、時間的な使用不可能領域64として把握する。なお、65はコンテンツの終了箇所である。

【0067】事業者側装置は現在時刻及びコンテンツの使用開始時刻を管理している。また、使用開始時刻を経過していれば、現在時刻から使用開始時刻を引いた値をコンテンツの先頭に足した時間的位置を、現在時刻における再生箇所と定義する。

【0068】図10に、事業者から加入者へコンテンツを配信する処理の流れを示す。事業者側装置11は、コンテンツを加入者側の記憶装置31あるいはその領域の一部に予め送信する（S1）。加入者側の記憶装置31は、受信（S2）後に暗号化されたコンテンツを記憶する（S3）。

【0069】図11に、加入者側端末がコンテンツの使用を要求する処理の流れを示す。加入者側の端末32から記憶装置31あるいはその領域の一部に要求を送信し（S11）、記憶装置31は受信後に事業者に要求信号を転送する（S12）。事業者は要求信号を受信し、加入者の認証を行った（S13）後に、コンテンツの使用許可を判定する（S14）。

【0070】次に、判定方法について述べる。

【0071】加入者側装置から要求する時間的位置が、図9に示したコンテンツの使用開始箇所62と現在時刻相当箇所61との間にあたる使用可能領域63を指定していれば許可する。また、それ以外の領域にあたる使用不可能領域64を指定していれば不許可とする。

【0072】コンテンツを早送りする場合の判定方法を図12に示す。

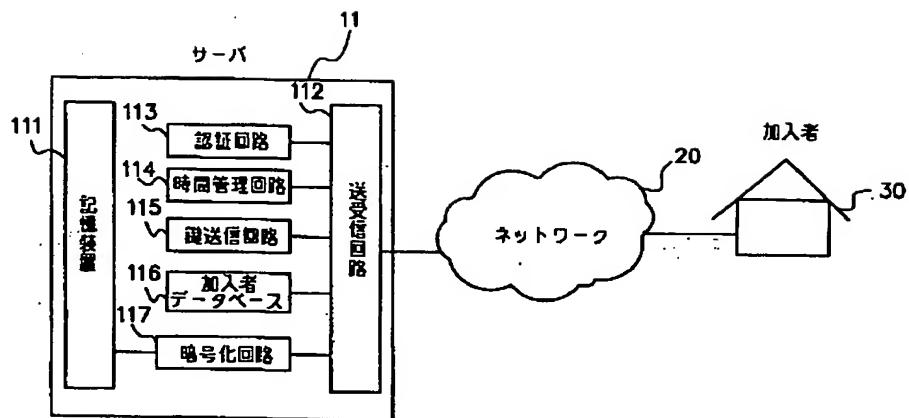
【0073】早送り箇所の指定は、コンテンツの先頭部分62からの時間的位置を指定する。事業者側装置は、現在時刻から使用開始時刻を引いた時間と、加入者側の装置が要求するコンテンツの先頭62からの時間的位置（現在の再生箇所）66とを比較し、前者の値が大きい場合は現在時刻相当箇所61よりも過去の領域を指定しており、事業者側の装置は早送り可能領域67と判定する。そして、許可を与え、コンテンツの暗号を解除する鍵を加入者側装置に送信する。

【0074】逆に、後者の値が大きければ、現在時刻相当箇所61よりも未来の部分を加入者側装置は要求しており、早送り不可能領域68と判定する。そして、事業者側の装置は加入者側装置に不許可を通知する。

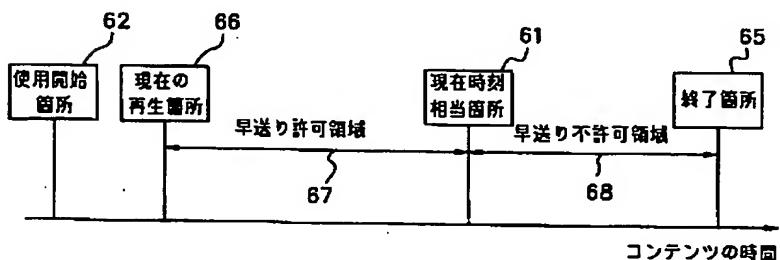
【0075】巻き戻しは時間的に過去の領域であり、事業者側はコンテンツの使用の許可を通知する。

【0076】これらの判定方法に従い、許可あるいは不許可を決定する。

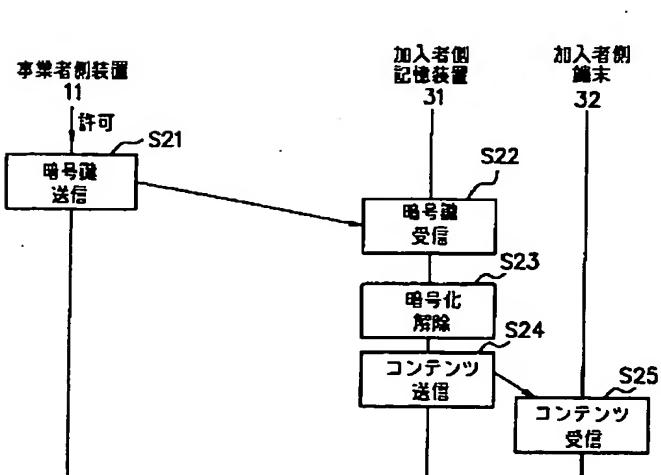
【図 8】



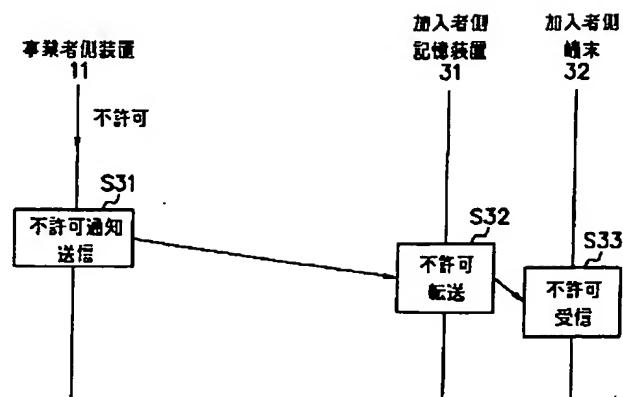
【図 12】



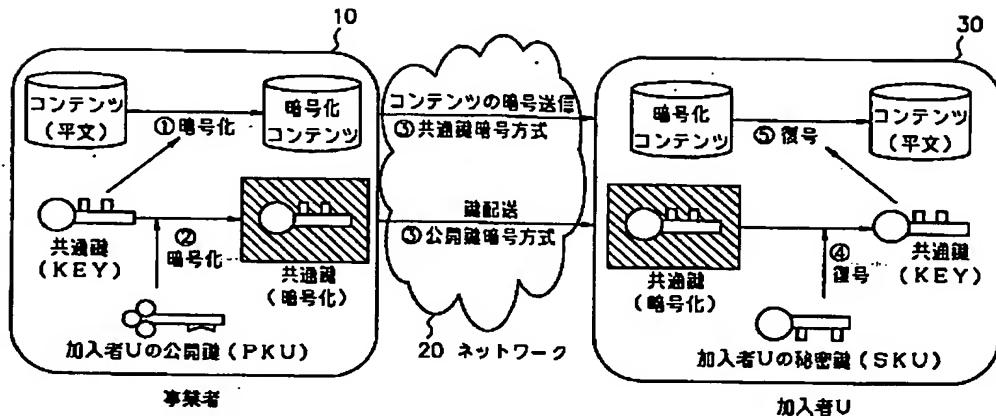
【図 13】



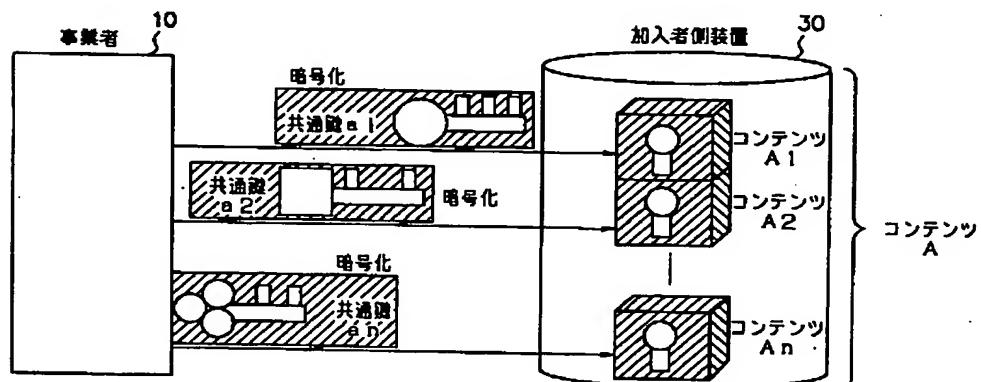
【図 14】



【図15】



【図16】



フロントページの続き

F ターム(参考) 5C064 BA01 BB02 BC06 BC17 BC18  
 BC22 BC23 BC25 BD02 BD08  
 BD09 CA01 CA14 CB01 CC01  
 5J104 AA12 AA16 BA03 EA06 EA19  
 NA02 PA07